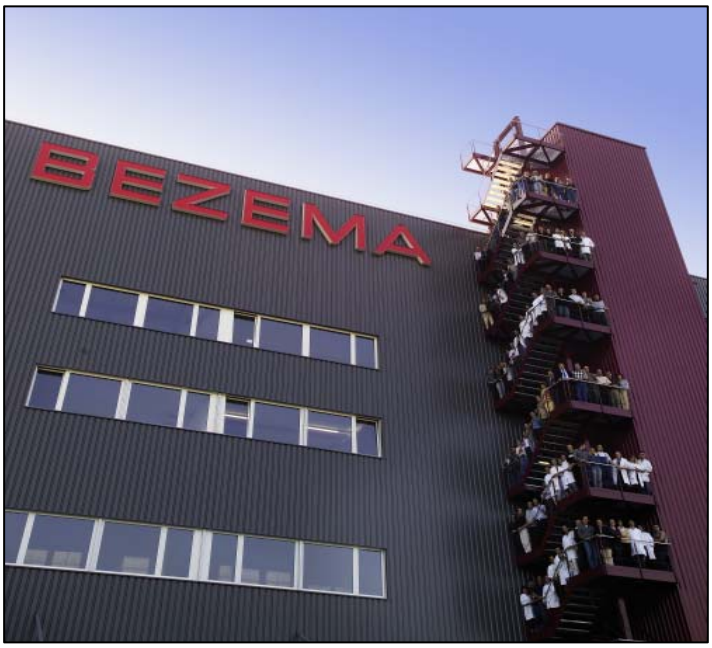
Bezema aumenta la sicurezza delle informazioni

Studio di riferimento IBM Security Network Intrusion Prevention System *della serie GX*

Cliente: Bezema AG, Montlingen

Bezema AG è un'azienda di Montlingen che fa parte del gruppo internazionale CHT. Fornisce prodotti innovativi e di elevata qualità ai clienti delle lavanderie industriali e della chimica edile. Ha sede nel Rheintal svizzero e abbraccia dunque tre Paesi: Svizzera, Austria e Germania. Si tratta di un'azienda di fama mondiale che costituisce un punto di riferimento per il settore tessile tradizionale.



"Grazie all'*IBM Security Appliance *siamo in grado di reagire immediatamente agli attacchi dei pirati informatici, di minimizzare i danni e di migliorare ulteriormente la sicurezza delle informazioni nella nostra azienda".

Peter Bossart, presidente di ICT Bezema AG

Highlights

- **Facile da integrare:** *IPS* è una soluzione tecnica che funziona come un ponte tradizionale e presso Bezema è stato possibile applicarla con estrema semplicità. Non si è nemmeno dovuta modificare l'architettura di rete già esistente.

- **Veloce da implementare:** è stato necessario soltanto un giorno di lavoro in sede per installare il pacchetto. Il *fine-tuning* dell'*IPS* è avvenuto in maniera remota tramite connessione VPN securizzata.

- **Elevata disponibilità:** grazie all'opzione *fail-open*, integrata nella serie GX, anche in caso di guasto dell'hardware installato si garantisce la disponibilità dell'infrastruttura del server.

- ***Reporting*:** la direzione riceve continuamente report tecnici sullo stato della sicurezza e sugli eventuali abusi e così è in grado di riconoscere il valore degli investimenti effettuati.

La sfida

Dopo un attacco da parte di pirati informatici nel 2009, la divisione *ICT* ha cercato di capire in che modo si potesse affrontare la situazione e come si potesse difendere in futuro.
Come per tante altre aziende erano previsti i tradizionali dispositivi di sicurezza, come i *firewall* e gli anti-virus sul desktop.
Ma non solo, presso Bezema oltre a quella principale si dovevano collegare altre due reti esterne per consentire ai diversi collaboratori dell'azienda di lavorare con i loro laptop da qualsiasi parte del mondo.
Per proteggere in modo efficiente un'infrastruttura di questo genere è stato necessario il contributo di tutti e un'attenta riflessione. Fin da subito è parso chiaro che in questa azienda non si trattava solo di eliminare la minaccia dei pirati informatici, ma anche di adottare provvedimenti per impedire in modo efficace possibili attacchi futuri.

La soluzione

Bezema ha così chiesto al Business Partner IBM Mips Computer AG di installare un *Intrusion Prevention System (IPS)*.

Oggi un sistema di questo tipo è in grado di riconoscere gli attacchi al sistema già a livello di protocolli e, contrariamente ai *firewall*, comprende il linguaggio utilizzato dai protocolli in uso (http, ftp, SMTP, ecc.). Se qualcuno ad esempio cerca di craccare una password con un *brute-force-attack,* l'*IPS* riconosce il pericolo, lancia l'allarme e blocca l'intruso.

È stato dunque installato questo sistema sul segmento perimetrale di Bezema. In tal modo viene controllato tutto il traffico di dati tra le reti esterne e quella principale e Internet.

L'*IPS* non è un sistema statico: man mano che le nuove conoscenze del team di ricerca *X-Force* di IBM confluiscono nel sistema il livello di sicurezza aumenta continuamente. Un sistema *IPS* ha bisogno di assistenza per poter funzionare in modo ottimale.

Bezema utilizza questa soluzione da circa un anno e in questi mesi sono già stati scoperti e scongiurati tempestivamente diversi attacchi.

I vantaggi della soluzione IPS Proventia GX

- **Riconosce e comprende più di 200 protocolli:** grazie alla tecnologia *X-Force* di IBM, l'attuale versione del modulo di analisi è in grado di comprendere più di 200 protocolli e di analizzare così tutto il traffico, reagendo opportunamente.
- **Protezione preventiva grazie alla tecnologia *Virtual Patch* di IBM:** protegge i sistemi in pericolo contrastando gli attacchi ai punti deboli del sistema. Così si guadagna tempo prezioso per testare e sviluppare aggiornamenti per la sicurezza e *patch* con cui si possono eliminare i punti deboli.
- **Sicurezza delle applicazioni web:** protegge le applicazioni web come server, negozi on-line e applicazioni 2.0 e offre lo stesso livello di sicurezza di un *firewall*.
- **Trasparente e invisibile (per i malintenzionati):** siccome il dispositivo di sicurezza è localizzaro al livello 2 del modello ISO/OSI, è possibile integrarlo facilmente in qualsiasi infrastruttura di rete già esistente.
- **Performance:** i diversi modelli consentono di analizzare i dati fino a un flusso di 8 Gbps, con un tempo di latenza di meno di 200 microsecondi.
- **Gestione centralizzata e *reporting*:** anche con la console di gestione "*Site Protector*" le soluzioni per la sicurezza di IBM possono essere gestite in modo centralizzato. Inoltre viene integrato uno strumento per il *reporting* estremamente efficiente.

Contatti:

IBM Schweiz
Markus Böck
Vulkanstrasse 106
Postfach
8010 Zürich

Mips Computer AG
Roger Schmid
Oberdorfstrasse 13
Postfach
6340 Baar